IN THE CLAIMS:

1. (Currently amended) A method in a data processing system for executing cryptographic operations, the method comprising:

responsive to a request to perform a cryptographic operation, dynamically selecting between one of a software process and a hardware process within the data processing system for performing the cryptographic operation based on a policy, to form a selected process; and

performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, and wherein the step of performing the cryptographic operation includes converting the key to a form useable by the selected process if the key is in an unusable form by the selected process, wherein the key is a software key and the selected process is the hardware process and the step of converting the key comprises converting the software key into a hardware form useable by the hardware process for performing the cryptographic operation.

2. (Original) The method of claim 1, wherein the policy includes selecting the one based on available resources to perform the cryptographic operation.

3. (Original) The method of claim 1, wherein the policy includes selecting the one resulting in a fastest completion of the cryptographic operation.

4. (Original) The method of claim 1, wherein the selecting step includes:

selecting the one using a preference associated with the request.

5-7. (Cancelled)

8. (Previously presented) A method in a data processing system for executing cryptographic operations, the method comprising:

responsive to a request to perform a cryptographic operation, dynamically selecting between one of a software process and a hardware process within the data

processing system for performing the cryptographic operation based on a policy, to form a selected process; and

performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, wherein the key is a hardware key and the selected process is the software process and further comprising:

converting the hardware key into a software form useable by the software process for performing the cryptographic operation.

9. (Currently amended) The method of claim ~~1~~ 8, wherein the policy comprises a set of rules used to minimize available resources consumed in performing the cryptographic operation.

10. (Currently amended) The method of claim ~~1~~ 8, wherein the policy comprises a set of rules used to maximize a speed at which the cryptographic operation is performed.

11. (Cancelled)

12. (Currently amended) The method of claim ~~11~~ 8, wherein the cryptographic operation is one of a message digest and a public-private key encryption.

13. (Currently amended) The method of claim ~~11~~ 8, wherein the request is received from an application.

14. (Original) The method of claim 13, wherein the request is received from the application using an application program interface call made by the application.

15-18. (Cancelled)

19. (Currently amended) The method of claim ~~11~~ 2, wherein the available resources include available processing resources and memory.

20-25. (Cancelled)

26. (Currently amended) A data processing system for executing cryptographic operations, the data processing system comprising:

selecting means for dynamically selecting between one of a software process and a hardware process within the data processing system for performing a cryptographic operation based on a policy, to form a selected process in response to a request to perform the cryptographic operation; and

performing means for performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, and wherein the performing means includes converting means for converting the key to a form useable by the selected process if the key is in an unusable form by the selected process, wherein the key is a software key and the selected process is the hardware process and the converting means comprises means for converting the software key into a hardware form useable by the hardware process for performing the cryptographic operation.

27. (Original) The data processing system of claim 26, wherein the policy includes selecting the one based on available resources to perform the cryptographic operation.

28. (Original) The data processing system of claim 26, wherein the policy includes selecting the one resulting in a fastest completion of the cryptographic operation.

29. (Original) The data processing system of claim 26, wherein the selecting means includes:

selecting means for selecting the one using a preference associated with the request.

30-32. (Cancelled)

33. (Currently amended) ~~The data processing system of claim 26~~ A data processing system for executing cryptographic operations, the data processing system comprising:

selecting means for dynamically selecting between one of a software process and a hardware process within the data processing system for performing a cryptographic operation based on a policy, to form a selected process in response to a request to perform the cryptographic operation; and

performing means for performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, and wherein the performing means includes converting means for converting the key to a form useable by the selected process if the key is in an unusable form by the selected process, wherein the key is a hardware key and the selected process is the software process and ~~further comprising:~~ the converting means comprises means for converting the hardware key into a software form useable by the software process for performing the cryptographic operation.

34. (Currently amended) The data processing system of claim ~~26~~ 33, wherein the policy comprises a set of rules used to minimize available resources consumed in performing the cryptographic operation.

35. (Currently amended) The data processing system of claim ~~26~~ 33, wherein the policy comprises a set of rules used to maximize a speed at which the cryptographic operation is performed.

36. (Cancelled)

37. (Currently amended) The data processing system of claim ~~36~~ 33, wherein the cryptographic operation is one of a message digest and a public-private key encryption.

38. (Currently amended) The data processing system of claim ~~36~~ 33, wherein the request is received from an application.

39. (Original) The data processing system of claim 38, wherein the request is received from the application using an application program interface call made by the application.

40-41. (Cancelled)

42. (Currently amended) ~~The data processing system of claim 36, wherein the key is a hardware key and the selected process is the software process and further comprising:~~

~~converting means for~~ A data processing system comprising:

a bus system;

a communications unit connected to the bus, wherein data is sent and received using the communications unit;

a memory connected to the bus system, wherein a set of instructions are located in the memory; and

a processor unit connected to the bus system, wherein the processor unit executes the set of instructions to (i) dynamically select between one of a software process and a hardware process within the data processing system for performing a cryptographic operation based on a policy, to form a selected process; (ii) perform the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, wherein the key is a hardware key and the selected process is the software process; and (iii) converting the hardware key into a software form useable by the software process for performing the cryptographic operation.

43. (Currently amended) ~~The data processing system of claim 36, wherein the key is a software key and the selected process is the hardware process and further comprising:~~

~~converting means for~~ A data processing system comprising:

a bus system;

a communications unit connected to the bus, wherein data is sent and received using the communications unit;

a memory connected to the bus system, wherein a set of instructions are located in the memory; and

a processor unit connected to the bus system, wherein the processor unit executes the set of instructions to (i) dynamically select between one of a software process and a hardware process within the data processing system for performing a cryptographic operation based on a policy, to form a selected process; (ii) perform the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, wherein the key is a software key and the selected process is the hardware process; and (iii) converting the software key into a hardware form useable by the hardware process for performing the cryptographic operation.

44-46. (Cancelled)